CLAIMS:

1. A transmission system for providing conditional access to transmitted data; the system including a transmitter and a plurality of receivers coupled via a network;

- the transmitter including means for transmitting:
  - to all receivers same data encrypted under control of a same authorization key; and
  - to all receivers a same key block with a plurality of entries, where each entry is associated with a respective different device key, at least some of the entries containing a representation of the authorization key encrypted with the associated device key, and
- the receiver being associated with a set of a plurality of device keys; the receiver including:
  - means for receiving the key block and the encrypted data;
  - a first decryptor for retrieving the authorization key by decrypting at least one entry of the key block that is associated with one of the set of device keys associated with the receiver; and
  - a second decryptor for decrypting the data under control of the authorization key.

2. A transmission system as claimed in claim 1, wherein the set of device keys associated with each respective one of the receivers is unique for the receiver.

3. A transmission system as claimed in claim 1, wherein the transmitter is operative to disable decryption of the data in a receiver by changing the authorization key and transmitting a key block wherein entries associated with device keys which are associated with a receiver to be revoked contain values other than the representation of the authorization key encrypted with the associated device key.

4. A transmission system as claimed in claim 3, wherein the transmitter is operative to re-enable decryption of the data in a disabled receiver by changing the

authorization key and transmitting a key block wherein at least one of the entries associated with device keys which are associated with a receiver to be revoked contains the representation of the authorization key encrypted with the associated device key.

5. A transmission system as claimed in claim 1, wherein the transmitter is operative to renew a set of device keys of a specific receiver by transmitting to the receiver a new set of device keys encrypted under control of a fixed device key that is unique for the receiver, and wherein the receiver is operative to receive a set of encrypted device keys, and the receiver includes a third decryptor for decrypting the set of encrypted device keys under control of a fixed device key that is unique for the receiver.

6. A transmission system as claimed in claim 1 for broadcasting real-time data.

7. A transmitter for use in a transmission system as claimed in claim 1, wherein the transmitter is coupled via a network to a plurality of receivers; the transmitter including means for transmitting:

- to all receivers a same key block with a plurality of entries, where each entry is associated with a respective different device key, at least some of the entries containing a representation of an authorization key encrypted with the associated device key, enabling the receivers to retrieving the authorization key by decrypting at least one entry of the key block that is associated with one of the set of device keys associated with the receiver; and
- to all receivers same data encrypted under control of a same authorization key, enabling the receivers to retrieve the data by decrypting the data under control of the authorization key.

8. A receiver for use in a transmission system as claimed in claim 1, wherein the receiver is associated with a set of a plurality of device keys; the receiver including:

- means for receiving encrypted data which is the same for all receivers in the system and which is encrypted under control of an authorization key which is the same for all receivers in the system;
- means for receiving a key block which is the same for all receivers in the system; the key block including a plurality of entries, where each entry is associated with a respective different device key, at least some of the entries containing a representation of the authorization key encrypted with the associated device key,

- a first decryptor for retrieving the authorization key by decrypting at least one entry of the key block that is associated with one of the set of device keys associated with the receiver;
- a second decryptor for decrypting the data under control of the authorization key.